

Dear FCC,

I wish to express a number of concerns regarding the report and order on Digital Broadcast Content Protection. Aside from the issue that I find the order to be ill-advised and unwarranted, there are a number of technical issues and contradictory claims in the report. I will outline these issues below:

1) The report fails to understand that the PC, as a general purpose computer, is under the control of the user, not the "PC manufacturer".

The PC simply cannot be lumped together with consumer electronic devices.

HDTV tuner modules are generally sold as after-market PCI cards and generally not installed by the PC manufacturer. The PC manufacturer has

no control over how these cards are used. Further, any bus on the PC,

including internal memory buses, cannot be considered secure as a user

may employ software debuggers and disassemblers to ascertain the precise

data being sent across such internal buses. There is no need for specialized equipment such as logic analyzers to examine these buses.

(Although, it should be pointed out, such equipment is readily available and it is little more difficult to monitor a memory bus than a PCI bus).

2) There is a general misunderstanding concerning the robustness of protection

systems. Particularly that closed source implementations are of a higher level of security than open source implementations. This assumption has been proven false many times through numerous security exploits of closed source systems.

The real measure of security in DRM protection systems is the ability to modify

and alter such systems, not whether or not the system is available in

source code form. Ultimately, any closed source system which is widely

deployed will likely be reversed engineered. On an open architecture

machine like the PC, there is little that can be done to prevent the

use or modification of such reverse-engineered information.

While an

"ordinary user" would not be able to make such modifications on their

own, an expert user can codify these modifications in his own program.

This program may be trivially and widely distributed over the Internet and

an "ordinary user" would certainly have no problem downloading and installing

such a program. This form of attack is known as "BORE" -- Break Once, Run

Everywhere. The PC, as an open architecture device, is widely subject

to such attacks with regard to PC software-only protection schemes.

Both open source and closed source embedded system's are secure by virtue of the fact that it can be verify difficult to modify the operation and output of such devices. Note that open source cryptography

employed in such devices is secure by virtue of the fact that the keys

are not considered part of the source. They are uniquely generated numbers

which are not shared with the source. It is has long been recognized that open cryptographic

algorithms which have been widely peer-reviewed are the most secure. Indeed,

NIST publishes such open algorithms for the use of the government, banking, and other industries.

3) The report fails to sufficiently define an "ordinary user" level of

robustness. Further, Section 73.9007 seemingly contradicts any reasonable definition of an "ordinary user". For example, almost any

PC software-based protection scheme would be subject to circumvention through

the use of debuggers and decompilers. Further, a number of consumer devices

would also be subject to circumvention by using a debugger to disassemble

their embedded code, an EPROM writer to burn a new ROM with altered embedded code, and a soldering iron to install the new ROM.

This is not a critique of the requirements in section 73.9007, only

the notion that this such levels of expertise somehow reflect the skills of an "ordinary user".

#### Recommendations:

1) The FCC needs to greatly clarify the definition of "ordinary user". I

suggest that any PC software-based protection be considered insecure due

to the "BORE" type attacks that allow circumvention via trivially downloaded

and installed software. Consumer devices should employ hardware-based

code-signing or "Secure" CPU's which include both ROM memory and the CPU

on the same chip die (thus preventing "chipping" of the system).

2) Allowing PC software-based protection mechanisms which rely on obscurity for security presents two major issues. Such a policy allows insecure and readily circumventable mechanisms to be deployed, and unfairly discriminates against PC's running open source operating systems.

It is suggested that the FCC adopt robustness requirements for PC-based systems which involve the use of embedded cryptography and video overlay technology. Such tuner modules encrypt content with a unique key. This key is not shared with the PC software, rather it is kept hidden within the PCI card's embedded software. The PC software may store the encrypted video stream on it's hard-drive, but cannot access the raw video. Only the tuner card itself may playback the video. A loopback connector is employed to overlay the analog video over the PC video output.

Such a system is both secure and fair to open source PC operating systems as the PC operating system is never allowed to handle the raw un-encrypted data stream. The operating system simply acts as a conduit to feed the encrypted stream back and forth to the hard-drive.

It should be noted that such a video card is already available on the market.

Namely, the accessDTV ([www.accessdtv.com](http://www.accessdtv.com)) HDTV PCI tuner card employs embedded cryptography and overlay video playback support via a loopback connector.

With further refinement, such a card could exchange it's key with other secure consumer devices using public-key cryptography. Again, the untrusted PC software would not be allowed to see the key in the clear, but rather it would merely act as a data conduit to pass the encrypted data between the two secure devices.

Such requirements should not be considered onerous as the majority of

HDTV viewers will likely use consumer-based devices (rather than open PC's) to process and view HDTV video. For the few who choose to use PC-based systems, it is not unreasonable to require that the solutions be both secure and fair (to open-source operating systems on the PC).